Exhibit 10

The future of data security: An interview with Dell Fellow Tim Brown

By Power More | November 16, 2015

By Kevin L. Jackson, CEO, GovCloud Network

The Dell Fellows program recognizes engineers for their outstanding and sustained technical achievements, engineering contributions and advancement of the industry. They are also seen as top innovators that have distinguished themselves through ingenuity, intellectual curiosity and inventiveness in the delivery of technology solutions. For these reasons and more, I couldn't pass up the opportunity to speak with Timothy G. Brown, Executive Director Security and Dell Fellow. During our broad-ranging discussion, Tim shared with me his exciting view of security in the not too distant future.

Kevin Jackson: Tim, I am very pleased to meet with you today. Thank you for taking the time.

Tim Brown: No problem Kevin, The pleasure is all mine.

Jackson: Before we look into your crystal ball, would you please explain your role at Dell?

Brown: Sure. I'm a Dell Fellow, one of eight Fellows across the company. We focus on looking at the future of technology and how we can innovate to make Dell better. My primary focus is on Dell security solutions.

Jackson: What has changed in the cybersecurity marketplace over the past 12 months?

Brown: There are many changes going on in the marketplace. Not only are the adversaries changing, but products and solutions for protecting enterprises are also changing quickly. In security, change is driven by those forces looking to gain access to our customer's data and information. That adversary is getting more focused, delivering more crimeware, perpetrating more targeted attacks and testing new criminal business models.

Jackson: Do these so-called adversaries operate as a business?

Brown: They absolutely do. These groups are running multi-billion dollar businesses with a main goal of keeping that money flowing. They continually make investments in finding new models. The cash flow from one of their current models, stealing credit cards and associated information, is now weening off due to effective actions across the credit card industry. Today's alternative payment models are making it much harder to turn credit cards into cash. This is why we now see things like ransomware. That is a harder type of attack but it has been effective in delivering more revenues. On the defensive side, analytics, more robust identity management and encryption are being more broadly used.

Jackson: What is the number one cybersecurity challenge facing your customers and partners today?

Brown: One of the biggest challenges is the lack of security professionals. There is negative unemployment in the field and companies are finding their openings very hard to fill. Five years ago, banks and large retailers employed most security professionals. Today every company in every industry needs them including your "mom and pop" corner store and the elementary school down the street. There are also technical challenges around selecting the right data protection software.

Jackson: So with the shortfall in cybersecurity professionals will Dell capitalize on the opportunity by becoming a security staffing agency over the next 12 months?

Brown: Maybe not a staffing agency but our industry leading managed security solution, SecureWorks, has actually helped our clients address their staffing shortfall. In fact, the rapid growth of SecureWorks is being primarily driven by that solution's ability to do the grunt work associated with monitoring the firewalls and networks. At the same time, we've developed advanced software that monitors and updates Sonicwall devices. Constantly done in the background, this ensures that the latest intrusion detection, anti-virus and malware signatures are always deployed. Secureworks, by the way, also has a staff augmentation offering.

Jackson: So Dell is reducing security staffing requirements through the use of advanced software.

Brown: Yes! We deliver intelligent software that can be deployed, managed and used efficiently by your existing staff. We are not telling you to buy our software and hire three more people because that doesn't work in today's environment.

Jackson: You seem to be approaching the problem just as your customers and partners would.

Brown: Gone are the days when if an enterprise had a problem, all they needed to do was to throw more people on it. Companies need to be judicious with their human assets so our solutions help organizations operate in a more efficient manner. We help your staff focus on the most pressing issues at hand. This allows you to apply human ingenuity to those issues that require it, leaving the mundane and business as usual stuff to the software. What's also surprising is the number of security "greenfields" we are seeing now. These are organizations that have not had any significant cybersecurity programs in the past and that are only now putting something in place. This has been more pronounced in education and healthcare industries.

Jackson: At Dell Peak Performance we heard that enterprises have suffered over $600B in cybersecurity losses this year against just a $200B investment to protect against these losses. What should senior decision makers and IT professionals learn from this statistic?

Brown: Organizations apply resources to those things that are important to them. In the past security just simply hasn't risen above the many other priorities. Even with new regulatory requirements in effect, companies are minimally applying resources. Instead of having these precious security resources being spread thinly across the enterprise we help organizations develop and deploy in a focused manner. This gives them more value for their dollar and actually can deliver better results than before. It's much easier to protect 50 things very strongly than it is to protect 5000 things weakly.

Jackson: With respect to cybersecurity, do you have any industry specific insights that you can share?

Brown: For me, healthcare immediately comes to mind because the industry as a whole is dealing with the challenges of electronic healthcare records. I was recently supporting a customer that had a data cable cut somewhere on their campus. Lack of access to electronic healthcare records prevented them from discharging patients for over 36 hours. So you can see how important securing that data while also maintaining redundant access is so important.

Healthcare records also need to be shared between multiple hospitals and multiple healthcare providers. This access must be managed and controlled so that privacy and

personally identifiable information is protected. From a commercial perspective, the healthcare industry will also be among the first industries dealing with the "internet of things". This is not only being driven by the changing nature of home healthcare and a rapid rise in the use of home healthcare monitoring devices, but also from the rising population of healthy seniors.

Imagine the value of an internet connected coffee pot owned by my parents, who are 87 and 89. In the very near future it could come on in the morning between 8:30 and 9:30 and send me an alert that everything is normal. To me, this coffee pot represents a non-invasive way of checking on them. If I don't get that notification in the morning, I'm immediately on a plane finding out what's wrong. These types of models can be integrated into the healthcare system, keeping the elderly healthy and more comfortable in their home. In this way healthcare and IOT will be both a showcase and a challenge when it comes to IT security.

Jackson: As a technologist dealing with the Internet of Things, healthcare information privacy and cross-border requirements share healthcare information, how do you deal with the different national and local laws?

Brown: National laws today are extremely difficult because they are based on data sovereignty rules. In some instances, these rules prevent the transportation of data outside a country's geographic border. To make this better, laws will probably need to be changed in some way and I believe that the use of software based encryption to protect information will be part of our future. From a regulatory perspective, this will require endpoint protection and approved processes for disassociating data access from system access. I can also imagine limited access to the encryption key which, with an individual's permission, would limit data access to one or two specified individuals. These types of enhancements require an ability to attach data access policies to the data itself. While no data protection silver bullets exist today, the next few years will be very interesting.

Jackson: Do you have any final comments or specific recommendations for corporate decision makers?

Brown: Today's data security landscape is less scary than it is exciting. Just think about all the things we can do better today than in the recent past. We can help the elderly stay healthy at home for a longer period of time and we can enable identity federation across many different companies. These capabilities create new opportunities and new business

models. Today's CEO therefore needs the right security partner. One that stands ready to answer the hard questions and ready to discover answers that embrace the new future of business.

Jackson: Thank you, Tim.

Brown: You're welcome, Kevin.

This post was written as part of the Dell Insight Partners program, which provides news and analysis about the evolving world of tech. Dell sponsored this article, but the opinions are my own and don't necessarily represent Dell's positions or strategies.